IN THE CLAIMS

Please amend the claims as follows:

1. (Currently Amended) A processor comprising:

a mechanism to identify memory as secure memory accessible by secure processes, and to identify non-secure memory accessible by both secure and non-secure processes; ~~and~~

a security enforcement mechanism to allow page tables for the non-secure processes to be stored in secure memory[[.]]; and

a translation look-aside buffer (TLB), wherein the security enforcement mechanism allows a page table access in secure memory while the processor remains in a non-secure mode after a TLB miss in a non-secure process.

2. (Canceled)

3. (Currently Amended) The processor of claim 1 wherein the security enforcement mechanism includes page table walk hardware capable of walking page tables in secure memory in response to architecture events other than TLB misses caused by non-secure processes.

4. (Original) The processor of claim 1 wherein the security enforcement mechanism includes circuits to differentiate between program generated memory accesses and architecture generated memory accesses, and to block program generated memory access from accessing secure memory.

5. (Canceled)

6. (Original) The processor of claim 1 further comprising virtual address translation hardware to perform virtual address translation for non-secure processes via page tables in secure memory.

7. (Canceled)

8. (Original) The processor of claim 1 further comprising a control register to specify whether page tables for non-secure processes are kept in secure memory or non-secure memory.

9. (Original) The processor of claim 1 further comprising page table walk hardware capable of accessing secure memory on behalf of non-secure processes.

10. (Currently Amended) A processor comprising:

an apparatus to differentiate between hardware generated memory accesses and software generated memory accesses and to grant secure memory access to hardware generated memory accesses[[.]];

wherein the hardware generated memory accesses are the result of a translation look-aside buffer (TLB) miss that occurs when the processor is running in a non-secure mode, and wherein the secure memory access occurs without the processor leaving the non-secure mode.

11-19. (Canceled)

20. (Currently Amended) A method comprising:

determining if a translation look-aside buffer (TLB) miss has occurred in a non-secure process running in a processor's non-secure mode;

determining if a current process page table is in secure or non-secure memory; and

if the current process page table is in secure memory, performing a page table walk in secure memory without leaving the non-secure mode.

21. (Canceled)

22. (Canceled)

23. (Original) The method of claim 20 further comprising if the current process page table is in non-secure memory, performing the page table walk in non-secure memory.

24. (Currently Amended) An electronic system comprising:

a plurality of antennas;

an amplifier coupled to at least one of the plurality of antennas to amplify communications signals;

a processor coupled to the amplifier; and

memory that can be partitioned by the processor into secure memory accessible by secure processes and non-secure memory accessible by secure or non-secure processes;

wherein the processor includes a security enforcement mechanism to allow page tables for non-secure processes to be stored in secure memory, and the processor includes a translation look-aside buffer (TLB), wherein the security enforcement mechanism allows a page table access in secure memory while the processor remains in a non-secure mode after a TLB miss in a non-secure process.

25. (Canceled)

26. (Currently Amended) The electronic system of claim 24 wherein the security enforcement mechanism includes page table walk hardware capable of walking page tables in secure memory in response architecture events other than TLB misses caused by non-secure processes.

27. (New) A processor comprising:

secure memory accessible when the processor is in a privileged secure mode or a user secure mode;

non-secure memory accessible when the processor is in a privileged non-secure mode or a user non-secure mode; and

a security enforcement mechanism that allows access to page tables in secure memory when a translation look-aside buffer (TLB) miss occurs in the user non-secure mode, wherein the access to the page table occurs without the processor leaving the user non-secure mode.

28. (New) The processor of claim 27 wherein the security enforcement mechanism is operable to allow access to page tables in secure memory when a translation look-aside buffer (TLB) miss occurs in the privileged non-secure mode, wherein the access to the page table occurs without the processor leaving the privileged non-secure mode.

29. (New) The processor of claim 27 further comprising a memory management unit to access the page table while the processor remains in the user non-secure mode.